INTERNET COMMUNICATIONS PRIVACY AFTER *UNITED STATES V. COUNCILMAN*

Theodore Y. McDonough[*]

I. INTRODUCTION

Over 169 million Americans use the Internet,[1] with about 92 million Americans going online during a typical day.[2] Of these, over 42 million send e-mail, over 9 million send an instant message, and nearly 1 million create a weblog.[3] E-mail, instant messaging, and weblogs are merely a few of the many ways in which individuals communicate over the Internet.[4] As use of the Internet as a means to communicate continues to grow, the lack of a comprehensive statute protecting the privacy of Internet communications exposes an ever-increasing number of individuals to online privacy threats.

To protect the privacy of their Internet activity, "individuals have historically relied on common law privacy principles and various pieces of non-comprehensive privacy-related legislation."[5] One statute frequently cited by those seeking to protect the privacy of their

[*] J.D., 2007, Seton Hall University School of Law; B.S., 2001, The Pennsylvania State University.

[1] *See* Pew Internet & American Life Project, *Demographics of Internet Users*, http://www.pewinternet.org/trends.asp (follow "Who's Online" hyperlink) (last visited May 16, 2007) (containing statistics detailing that seventy percent of people over age eighteen use the Internet); U.S. Census Bureau, Annual Estimates of the Population by Sex and Five-Year Age Groups for the United States: April 1, 2000 to July 1, 2005, http://www.census.gov/popest/national/asrh/NC-EST2005/NC-EST2005-01.xls (presenting population estimates in five-year age groups).

[2] Pew Internet & American Life Project, *Daily Internet Activities*, http://www.pewinternet.org/trends.asp (follow "Daily Activities" hyperlink) (last visited May 16, 2007).

[3] *Id.*

[4] *See, e.g.*, Sharon Housley, *E-mail, Instant Messaging, Blogs, RSS, Forums and Listservs: What's Next?*, Oct. 7, 2004, http://www.webpronews.com/topnews/2004/10/07/ email-instant-messaging-blogs-rss-forums-and-listservs-whats-next.

[5] Yonatan Lupu, *The Wiretap Act and Web Monitoring: A Breakthrough for Privacy Rights?*, 9 VA. J.L. & TECH. 3, ¶ 5 (2004), http://www.vjolt.net/vol9/issue1/v9i1_a03-Lupu.pdf.

Internet communications is the Crime Control and Safe Streets Act of 1968 ("Wiretap Act," or "the Act").[6] Amended by the Electronic Communications Privacy Act of 1986 (ECPA),[7] section 2511 of the Wiretap Act provides a private right of action "against certain interceptions of electronic communications."[8] These statutes, however, were written prior to public adoption of Internet communication, and their language fails to adequately address concerns regarding the privacy of Internet communications.[9]

As new technologies emerge, new laws must be drafted to specifically address the technology.[10] Unfortunately, the speed at which legislation can be enacted cannot match that at which new technologies are introduced. As new means of Internet communication are introduced, the lack of a statute written specifically to protect the privacy of these communications results in uncertainty about exactly what privacy protections these communications will be afforded.[11] Furthermore, recent court rulings suggest that current law is inadequate to protect the privacy of Internet communications.[12]

This Comment examines cases that addressed the level of privacy protections given to Internet communications, focusing on a recent case from the United States Court of Appeals for the First Circuit that examined whether an Internet Service Provider (ISP) could intercept its subscribers' e-mail messages without their knowledge or consent.[13] Although the court concluded that such an act was a violation of the Wiretap Act,[14] this Comment suggests that the decision will have little impact in protecting the privacy of Internet communications, in part because of amendments to the Wiretap Act made by the Uniting and Strengthening America by Providing Appropriate Tools Required to

[6] 18 U.S.C. §§ 2510–2522 (2000).

[7] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

[8] Lupu, *supra* note 5, ¶ 5.

[9] *See id.* n.9; *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1558 (2004) (noting that in 1986, when the ECPA was enacted, "relatively few people had Internet access; commercial electronic mail services . . . were emerging, but . . . primarily served the business community.").

[10] *See generally* Jay Campbell, *Protecting the Future: A Strategy for Creating Laws Not Constrained by Technological Obsolescence*, 7 VAND. J. ENT. L. & PRAC. 533, 539–40 (2005) (suggesting that current wiretapping laws are ill-suited to protect the privacy of Internet communications).

[11] *See id.* at 541.

[12] *See infra* Parts II.B.2–3.

[13] United States v. Councilman (*Councilman II*), 418 F.3d 67 (1st Cir. 2005) (en banc).

[14] *Id.* at 79.

Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).[15] Part II will introduce the Wiretap Act and relevant amendments that resulted from the ECPA. Part II will also discuss earlier attempts by individuals to use the Wiretap Act to protect the privacy of their Internet communications. Part III will discuss *United States v. Councilman*,[16] briefly recounting the case's history, and focusing on the court's en banc decision. Part IV discusses the practical effects the decision is likely to have in protecting the privacy of Internet communications, ultimately concluding that the decision will have no substantial impact on Internet communication privacy. Finally, Part V suggests ways in which Internet communication privacy could be increased.

In *United States v. Councilman*, the United States Court of Appeals for the First Circuit recently considered whether the Wiretap Act's protections applied to e-mails stored on an ISP's server.[17] A panel of the court, in *Councilman I*, initially construed the Wiretap Act so narrowly that it afforded practically no protection at all to e-mail and other Internet communications.[18] The panel decision prompted outcry and criticism from privacy advocates who saw the decision as eviscerating what little privacy protections existed for Internet communications.[19] At rehearing en banc, the court, in *Councilman II*, reversed the earlier panel decision, and held that e-mails in transient storage were indeed protected under the Wiretap Act.[20]

The en banc decision "restore[d] the law to what most had assumed it meant: unauthorized access to e-mail before it arrives in the customer's in-box is an interception covered by the Wiretap Act."[21] However, this restoration may not be permanent.

---

[15] *See infra* notes 103–07 and accompanying text.

[16] 418 F.3d 67 (*Councilman II*) (1st Cir. 2005) (en banc). The earlier panel decision in *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004), will be referred to as *Councilman I*, and the later en banc decision as *Councilman II*.

[17] *Id.* at 69–71.

[18] United States v. Councilman (*Councilman I*), 373 F.3d 197 (1st Cir. 2004), *rev'd en banc*, 418 F.3d 67 (1st Cir. 2005).

[19] *See, e.g.*, 150 CONG. REC. S7893–96 (daily ed. July 9, 2004) (statement of Sen. Leahy). Senator Leahy commented that "[i]f allowed to stand . . . [the panel decision] threaten[ed] to eviscerate Congress's careful efforts to ensure that privacy is protected in the modern information age." *Id.* at S7893.

[20] *Councilman II*, 418 F.3d at 69, 73.

[21] Center for Democracy & Technology, *Federal Appeals Court Reaffirms E-Mail Privacy Protections*, Policy Post 11.20 (Aug. 17, 2005), *available at* http://www.cdt.org/publications/policyposts/2005/20 [hereinafter Center for Democracy & Technology].

II. THE WIRETAP ACT

A. History of the Wiretap Act

Enacted by Congress in 1968, the Wiretap Act was largely a codification of the Supreme Court's holdings in *Berger v. New York*[22] and *Katz v. United States*.[23] The Wiretap Act was intended to "encourag[e] the uninhibited exchange of ideas and information among private parties."[24] Among other things, the Wiretap Act makes it illegal to intercept or conspire to intercept "any wire, oral, or electronic communication."[25]

As electronic communication technology advanced, the Wiretap Act was unable to adequately address these technological improvements.[26] Congress amended the Wiretap Act in 1986 to cover "the latest in electronic communication technology" by enacting the ECPA.[27] The ECPA is divided into two parts: the Wiretap Act[28] and the Stored Communications Act.[29] The ECPA "generally extend[ed] the prohibitions on interception to e-mail and craft[ed] new protections for stored communications and stored records held by third parties."[30]

Despite its best intentions, Congress could not anticipate advances in Internet communications when the ECPA was enacted.[31] "The words 'Internet,' 'World Wide Web,' and 'e-commerce' appear in neither the ECPA nor its legislative history."[32] Additionally, the ECPA "seemed particularly focused on the threat posed by police surveillance and [was] intended to . . . specify permissible uses of new technology by law enforcement."[33] Modern Internet communication

---

[22] 388 U.S. 41, 51–53 (1967) (explaining that Fourth Amendment protections applied to electronic interception of oral communications).

[23] 389 U.S. 347, 352 (1967) (holding that Fourth Amendment protections applied to telephone conversations).

[24] Bartnicki v. Vopper, 532 U.S. 514, 532–53 (2001) (quoting Brief of Petitioner-Appellant, United States, at 27).

[25] 18 U.S.C. § 2511(1)(a) (2000).

[26] *See* Mulligan, *supra* note 9, at 1561–64.

[27] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[28] 18 U.S.C. §§ 2510–2522 (2000).

[29] 18 U.S.C. §§ 2701–2712 (2000 & Supp. II 2003).

[30] Mulligan, *supra* note 9, at 1564.

[31] *See* Lupu, *supra* note 5, ¶ 9.

[32] *Id.*

[33] *Id.* Lupu notes that:

> [t]he Senate report begins with Justice Brandeis' famous quote from *Olmstead v. United States* . . . : "Ways may some day be developed by which the Government, without removing papers from secret drawers,

has made the laws protecting the privacy of communication obsolete once again, and

> [d]espite continuous calls for a definitive legislative stance on the protection of [Internet communication], Congress has not enacted a comprehensive statute. As a result, [individuals who claim their Internet communications have been illegally intercepted] have often relied on broad privacy-related statutes such as the Wiretap Act and the ECPA.[34]

The term "electronic communication" is broadly defined in the ECPA as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[35] Although the definition would seem to include nearly all forms of Internet communication, courts have found that the technical nature of these communications often precludes the extension of Wiretap Act protections to the Internet.[36]

B. Use of the Wiretap Act to Protect Internet Communication Privacy

Since the enactment of the ECPA and its consequential amendment to the Wiretap Act, relatively few courts have interpreted the statute's definition of "intercept." The ECPA has been described as "fraught with trip wires,"[37] and "famous (if not infamous) for its lack of clarity."[38] The definitions adopted by courts having had an opportunity to interpret this term suggest that these characterizations are accurate.

1. *Steve Jackson Games, Inc. v. U.S. Secret Service*[39]

More than a decade ago, the United States Court of Appeals for the Fifth Circuit considered whether e-mails in electronic storage

---

> can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?"

Id. at ¶ 9 n.22 (citing S. REP. NO. 99-541, at 2 (1986) (citing Olmstead v. United States, 277 U.S. 438, 474 (1928))).

[34] *Id.* ¶ 7.

[35] 18 U.S.C. § 2510(12) (2000).

[36] *See infra* Part II.B.

[37] Forsyth v. Barr, 19 F.3d 1527, 1543 (5th Cir. 1994).

[38] Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

[39] 36 F.3d 457 (5th Cir. 1994).

could be intercepted within the meaning of the Wiretap Act.[40] In *Steve Jackson Games, Inc. v. U.S. Secret Service*, the court considered

> whether the seizure of a computer, used to operate an electronic bulletin board system, and containing private electronic mail which had been sent to (stored on) the bulletin board, but not read (retrieved) by the intended recipients, constitute[d] an unlawful intercept under the Federal Wiretap Act as amended by [the ECPA].[41]

In concluding that the Wiretap Act had not been violated, the court focused on the distinction between the definitions of "wire communication" and "electronic communication" as set forth in the Act.[42]

Steve Jackson Games, Inc., published books, magazines, games, and related products.[43] The company also operated an electronic bulletin board service (BBS), where it "post[ed] information about its business, games, [and] publications."[44] The BBS also allowed customers "to send and receive private e-mail."[45] Until customers read their mail, it was temporarily stored on the hard drive of the BBS.[46]

During the course of an investigation into the unauthorized distribution of a text file containing information on Bell South's emergency call system, the Secret Service seized a computer used to operate the BBS.[47] Secret Service employees later read and deleted unread e-mails stored on the BBS.[48] However, the court found that the e-mails were not protected electronic communications and the Secret Service, therefore, did not violate the Wiretap Act by reading and deleting them.[49] The court stated:

> The E-mail in issue was in "electronic storage". Congress' use of the word "transfer" in the definition of "electronic communication", and its omission in that definition of the phrase "any electronic storage of such communication" (part of the definition of "wire communication") reflects that Congress did not intend for

---

[40] *Id.*

[41] *Id.* at 458 (internal citations omitted).

[42] *Id.* at 461–62.

[43] *Id.* at 458 (citation omitted).

[44] *Id.*

[45] *Steve Jackson Games, Inc.*, 36 F.3d at 458.

[46] *Id.*

[47] Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 435 (W.D. Tex 1993).

[48] *Steve Jackson Games, Inc.*, 36 F.3d at 459.

[49] *Id.* at 461–62.

> "intercept" to apply to "electronic communications" when those communications are in "electronic storage".[50]

This early decision made clear that certain forms of Internet communication might not be protected under the Wiretap Act.

2. *Konop v. Hawaiian Airlines*[51]

In *Konop v. Hawaiian Airlines*, the United States Court of Appeals for the Ninth Circuit considered whether an employer's unauthorized viewing of an employee's private, password-protected website was an "interception" in violation of the Wiretap Act.[52] The court adopted a narrow definition of "intercept," and held that, because it was in electronic storage, the website was not "intercepted" and there was no violation of the Wiretap Act.[53]

Konop, a pilot for Hawaiian Airlines, operated a website on which he "posted bulletins critical of his employer . . . and the incumbent union."[54] By requiring visitors to the site to create a user name and password, Konop controlled access to the site and created a list of individuals eligible to access the site.[55] A member of his employer's management team, a class explicitly prohibited from viewing the site by the site's terms and conditions, accessed the site by using the user names and passwords of two authorized users (with their permission).[56] The court held that "for a website . . . to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."[57] Finding Konop's website to be a stored electronic communication, the court concluded that the unauthorized access was not a violation of the Wiretap Act.[58] The court's reasoning suggests that current law is ill-suited to meaningfully protect the privacy of Internet communications.

3. *United States v. Steiger*[59]

The United States Court of Appeals for the Eleventh Circuit has also adopted a narrow interpretation of the Wiretap Act based on the

---

[50] *Id.*
[51] 302 F.3d 868 (9th Cir. 2002).
[52] *Id.* at 872–74.
[53] *Id.* at 878.
[54] *Id.* at 872.
[55] *Id.*
[56] *Id.* at 873.
[57] *Konop*, 302 F.3d at 878.
[58] *Id.*
[59] 318 F.3d 1039 (11th Cir. 2003).

reasoning of the Fifth and Ninth Circuits. In *United States v. Steiger*, the court noted that "very few seizures of electronic communications from computers will constitute 'interceptions.'"[60] The court quoted a scholarly work whose author identified a single circumstance when e-mail may be intercepted:

> There is only a narrow window during which an E-mail interception may occur—the seconds or mili-seconds [sic] before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.[61]

Whether under even these circumstances the Wiretap Act would be found to protect e-mail communications is an issue strikingly similar to the facts presented in a recent First Circuit case.[62]

III. *UNITED STATES V. COUNCILMAN*

In *United States v. Councilman*,[63] the United States Court of Appeals for the First Circuit considered whether the Wiretap Act applied to e-mail communications in temporary storage on the server of an e-mail service provider.[64] Bradford Councilman was a vice president of Interloc, an online literary clearinghouse that provided lists of rare and out-of-print books.[65] Interloc provided its customers with an e-mail address and was also the service provider.[66] The indictment alleged that Councilman instructed Interloc employees to write a computer program that would intercept all incoming e-mails to Interloc customers from Amazon.com and forward a copy to a mailbox

[60] *Id.* at 1050.

[61] *Id.* (quoting Jarrod J. White, Commentary, *E-mail@Work.com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079, 1083 (1997)) (second brackets in original).

[62] Although the technological issues in *United States v. Councilman* are similar to those in *Steve Jackson Games, Inc.*, *Konop*, and *Steiger*, it should be noted that the conduct complained of in the latter three cases was carried out using employers' resources and fell within the scope of the employment relationship, thereby potentially exposing the employers to liability. This likely influenced the courts' reasoning in those cases.

[63] United States v. Councilman (*Councilman II*), 418 F.3d 67 (1st Cir. 2005) (en banc).

[64] *Id.* at 67. The Wiretap Act was amended in relevant respects in 2001, whereas Councilman's alleged conduct occurred in 1998. Therefore, all cites to statutes in the court's opinion are to those in effect in 1998.

[65] *Id.* at 70.

[66] *Id.*

that Councilman could access.[67] Councilman routinely read these e-mails to gain a commercial advantage.[68]

Councilman contended that his conduct did not violate the Wiretap Act and moved to dismiss the indictment.[69] Because the e-mails were in "electronic storage"[70] when copied, Councilman argued, they could not be "intercepted" as a matter of law.[71] Initially, the district court denied Councilman's motion to dismiss,[72] but reconsidered its decision in light of *Konop*, which at that time had been recently decided.[73] The district court found that, at the moment they were copied, the e-mails were in "electronic storage" and therefore not subject to the Wiretap Act's prohibition on interception. The court agreed with Councilman's position and accordingly dismissed one count of the two-count indictment.[74]

On appeal, a divided panel of the court of appeals affirmed, concluding "that, because the definition of 'wire communication' includes 'electronic storage' but the definition of 'electronic communication' does not, the Wiretap Act's prohibition on 'intercept[ion]' does not apply to messages that are, even briefly, in 'electronic storage.'"[75] In his dissent Judge Lipez warned that the "line that we draw in this case will have far-reaching effects on personal privacy and security."[76] The full court later granted the government's petition for rehearing en banc.[77]

At the en banc rehearing, the *Councilman II* court stated that Councilman's argument raised questions of statutory construction[78] and began its analysis by introducing the history and scope of the

---

[67] *Id.*

[68] *Id.*

[69] *Councilman II*, 418 F.3d at 71.

[70] "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (1994).

[71] *Councilman II*, 418 F.3d at 71.

[72] United States v. Councilman, 245 F. Supp. 2d 319, 320 (D. Mass. 2003).

[73] *Id.*

[74] *Id.* at 321.

[75] *Councilman II*, 418 F.3d at 71 (citing United States v. Councilman (*Councilman I*), 373 F.3d 197, 200–04 (1st Cir. 2004)).

[76] *Councilman I*, 373 F.3d at 208 (Lipez, J., dissenting).

[77] United States v. Councilman, 385 F.3d 793 (1st Cir. 2004) (per curiam) (granting rehearing en banc, withdrawing the panel opinion, and vacating the judgment). As discussed *infra*, the full court of appeals later reversed the panel decision.

[78] *Councilman II*, 418 F.3d at 69.

Wiretap Act.[79] The court then proceeded to address the arguments by discussing the Wiretap Act's text, structure, and legislative history.[80]

First addressing the term "electronic communication," the court initially noted that the term's statutory definition appeared broad enough to include e-mail messages processed by a mail transfer agent (MTA).[81] The Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects commerce, but does not include – (A) any wire or oral communication."[82] Councilman argued that, when read together with the Act's definition of "wire communication," the scope of the definition of "electronic communication" would be limited by what the former includes but the latter does not.[83] The Act defined "wire communication" as:

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce *and such term includes any electronic storage of such communication.*[84]

Because the definition of "wire communication" included the phrase "and such term includes any electronic storage of such communication," while the definition of "electronic communication" did not, Councilman argued that "Congress intended wire communications, but not electronic communications, to include electronic storage."[85] The court also noted that the Act's definition of "electronic storage" included "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[86]

Councilman based his inference on a canon of construction—*expressio unius est exclusio alterius* (the express mention of one thing excludes all others)—and suggested that "where Congress includes particular language in one section of a statute but omits it in another

---

[79] *Id.* at 72.
[80] *Id.*
[81] *Id.* at 73.
[82] 18 U.S.C. § 2510(12)(A) (1994).
[83] *Councilman II*, 418 F.3d at 73.
[84] 18 U.S.C. § 2510(1) (1994) (emphasis added).
[85] *Councilman II*, 418 F.3d at 73.
[86] *Id.* (quoting 18 U.S.C. § 2510(17) (1994)).

section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."[87] Addressing whether Councilman's inference was justified, the court presented circumstances in which use of the canon is appropriate.[88] Because the sections' "language, structure, or circumstances of enactment"[89] differed, the court determined that the canon's application did not resolve the issue of whether electronic communications included electronic storage.[90]

Turning to the Act's legislative history, the court discussed the changes to the Wiretap Act that resulted from the passage of the ECPA.[91] At issue was the ECPA's amendment of the definition of "wire communication," to which the language "and such term includes any electronic storage of such communication" was added.[92] Based on the ECPA's legislative history, the court concluded that the electronic storage clause was added to the definition of "wire communication" for the sole purpose of regulating access to voice mail, not to remove electronic communications in temporary storage from the purview of the Wiretap Act.[93]

The court of appeals concluded that neither the text of the Wiretap Act nor its legislative history supported Councilman's argument that there was a distinction between e-mails "in transit" and "in storage."[94] But while the *Councilman II* court's opinion extends the protections of the Wiretap Act to e-mail messages prior to their arrival on the computer of the e-mail service provider, its limited scope

---

[87] *Councilman II*, 418 F.3d at 73 (quoting the Supreme Court's explanation of the canon in Russello v. United States, 464 U.S. 16, 23 (1983)).

[88] *Id.* at 74–75. The court stated that the *expressio unius* maxim is "most apt when Congress enacts a new, self-contained statute, and two provisions of that act, drafted with parallel language, differ in that one provision uses a term, but the other provision, where it would be equally sensible to use that term if Congress desired it to apply, conspicuously omits it." *Id.* at 74.

[89] *Id.* at 74.

[90] *Id.* at 76.

[91] *Id.* at 76–77. The ECPA was first introduced in 1985. After the Department of Justice expressed concern that e-mail would be given too much protection under the original ECPA, a new version that met some of the concerns was introduced the following year. *Councilman II*, 418 F.3d at 77.

[92] *Compare* 18 U.S.C. § 2510(1) (1982), *with* 18 U.S.C. § 2510(1) (Supp. IV 1986) (The 1986 amendments to the definition of "wire communication" added the electronic storage clause, "and such term includes any electronic storage of such communication.").

[93] *Councilman II*, 418 F.3d at 78–79.

[94] *Id.* at 79.

does little to resolve larger privacy questions concerning Internet communications.[95]

IV. *COUNCILMAN'S* EFFECT ON THE PRIVACY OF INTERNET COMMUNICATIONS

Essentially, the First Circuit's en banc decision does little more than "restore[] the law to what most had assumed it meant: unauthorized access to e-mail before it arrives in the customer's in-box is an interception covered by the Wiretap Act."[96] Moreover, this perceived restoration may not be long-lived.

A. Spyware, Spam, and E-mail as a "Stored Communication"

All major webmail services automatically scan incoming e-mail messages for viruses and spam. The overwhelming majority of webmail subscribers likely understand the need for this practice, and this Comment does not suggest that the practice be discontinued. However, without an exception in the Wiretap Act for such a practice, *Councilman II* would seem to make this practice illegal. Recognizing the need for these scans, the Wiretap Act contains an exception for providers of electronic communication services. Section 2511(2)(a)(i) allows "provider[s] of wire or electronic communication service . . . to intercept . . . [wire or electronic] communication[s] . . . [when necessary] . . . to the rendition of . . . service or to the protection of the rights or property of the provider of that service."[97] Scanning e-mails for viruses and spam undoubtedly falls under this exception.

However, the *Councilman II* decision does nothing to close the loophole in the Stored Communications Act that allows ISPs to read and use e-mails after they have reached the recipient's inbox. After an e-mail is delivered to a subscriber's inbox, it ceases to be an "electronic communication" protected by the Wiretap Act, and instead becomes a "stored electronic communication" afforded the lesser protections of the Stored Communications Act.[98] The provider of an e-mail service may, without restriction, read and use, but not disclose, the contents of any stored e-mail.[99] Whether an e-mail ceases to be an electronic communication "in transit" at a point earlier than when ac-

---

[95] *See, e.g.*, Center for Democracy & Technology, *supra* note 21.

[96] *Id.*

[97] 18 U.S.C. § 2511(2)(a)(i) (2000).

[98] *See, e.g.*, Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1222–23 (2004).

[99] *See* 18 U.S.C. §§ 2701–2702 (2000).

tually read by its intended recipient is an issue that the courts have yet to address.

Most major ISPs expressly disavow reading their subscribers' e-mails.[100] Nevertheless, "the gap in the law should be closed to reflect the norm."[101] As was suggested by the Center for Democracy and Technology, "ISPs should only be allowed to read and use their customers' e-mail when necessary to protect the ISPs' rights or enforce the terms or service, or with prior informed consent, which is the rule that has always been applicable to voice communications."[102]

Additionally, the USA PATRIOT Act[103] might have a substantial impact on the effect of *Councilman II*. Section 209 of the act amended the definition of wire communication by removing the language "and such term includes any electronic storage of such communication."[104] Although this amendment was intended to remove voice mail from the protection of the Wiretap Act, it also weakens perhaps the most logical argument in support of extending Wiretap Act protections to e-mail in transit. Specifically, if voice mail were afforded the protections of the Wiretap Act, it would be illogical to treat e-mail in transit disparately.

Although courts have not yet specifically addressed section 209's effect on the interception of e-mail messages in transit, the *Konop* opinion is helpful in evaluating the amendment's potential consequences. In *Konop*, the United States Court of Appeals for the Ninth Circuit noted that "[b]y eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of 'intercept'—acquisition contemporaneous with transmission—with respect to wire communications."[105] Furthermore, the court suggested that when the USA PATRIOT Act was passed, "Con-

[100] *See, e.g.*, Gmail Terms of Use, http://gmail.google.com/gmail/help/terms_of_use.html (last visited Apr. 5, 2007) (Section 8 states that "[n]o human will read the content of your e-mail . . . without your consent"); *see also* Saul Hansell, *You've Got Mail (and Court Says Others Can Read It)*, N.Y. TIMES, July 6, 2004, at C1.

[101] Center for Democracy & Technology, *supra* note 21.

[102] *Id.*

[103] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered titles and sections of 8, 15, 18, 22, 31, 42, 49, and 50 U.S.C.).

[104] *Compare* 18 U.S.C. § 2510(1) (2000) (defining the term wire communication to include "electronic storage of such communication"), *with* 18 U.S.C. § 2510(1) (Supp. I 2001) (defining the term wire communication, from which the clause "and such term includes any electronic storage of such communication" has been deleted).

[105] Konop v. Hawaiian Airlines, 302 F.3d 868, 878 (9th Cir. 2002).

gress . . . was aware of the narrow definition courts had given the term 'intercept' with respect to electronic communications"[106] and by choosing not to modify that definition, "Congress . . . accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission."[107] If correct, this reasoning suggests that an ISP may intercept e-mail messages en route from sender to recipient, while those messages are in transient storage, without a violation of the Wiretap Act.

B. Gmail

Shortly after Google's April 1, 2004, announcement of its release of Gmail, the service was criticized by privacy groups as breaching wiretapping laws and exposing users to increased threats to privacy.[108] Two aspects of Gmail are of particular concern, but on only one might *Councilman II* have a significant impact.[109] Specifically, Google's use of Adsense technology, which scans messages in order to deliver targeted advertisements and related information, may, after *Councilman II*, be an "interception" in violation of the Wiretap Act.[110]

Gmail uses Adsense, the same program that places text advertisements on Google search result pages, to scan e-mails upon viewing and deliver targeted advertisements based on the content of the e-mail.[111] This advertising subsidizes the cost of the service, and many users are willing to accept this practice in return for free service.[112]

---

[106] *Id.*

[107] *Id.*

[108] *See, e.g.*, Hansell, *supra* note 100, at C1; Press Release, Thirty-one Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail (Apr. 19, 2004), *available at* http://www.privacyrights.org/ar/GmailLetter.htm (urging suspension of Gmail service until privacy issues are adequately addressed).

[109] The second aspect of concern is Gmail's 2.5-gigabyte storage capacity, which allows the average subscriber to store e-mails indefinitely, as storage space is no longer an issue. Thorough discussion of this concern, however, is beyond the scope of this Comment, as it has little to do with the *Councilman II* decision and existed before Gmail's introduction. For an analysis and discussion of the concerns associated with Gmail's storage capacity, see Brad Templeton, *Privacy Subtleties of GMail*, http://www.templetons.com/brad/gmail.html (last visited May 18, 2007).

[110] *See* About Gmail, http://gmail.google.com/gmail/help/about_privacy.html (last visited May 18, 2007).

[111] *See* About Gmail: Are There Ads in Gmail?, http://mail.google.com/mail/help/about.html (last visited May 18, 2007); What's Adsense, http://www.google.com/services/adsense_tour/index.html (last visited May 18, 2007).

[112] Google has declined to report exactly how many subscribers Gmail currently has, revealing "only that there [are] millions." Laurie J. Flynn, *Google Links Chat and Mail Services*, INT'L HERALD TRIB., Feb. 8, 2006, at 16.

However, after *Councilman II*, this practice may be in violation of the Wiretap Act.

As discussed above, scanning e-mail for spam is undoubtedly a "necessary incident to the rendition of . . . [e-mail] service,"[113] and service providers may properly intercept e-mail messages for those purposes. Additionally, there are few technical differences between scanning for spam and scanning to deliver targeted advertisements.[114] But courts have yet to decide whether scanning to deliver targeted advertisements can be considered a "necessary incident to the rendition of . . . [e-mail] service."[115]

While subscribers to Gmail consent to have their e-mails scanned as part of the service's terms of use, those who send e-mail to Gmail accounts have not done so, and those e-mails are being scanned as well.[116] It is this scanning of e-mail from non-consenting persons that is of particular concern.

Whether Wiretap Act protections apply to e-mails from non-consenting correspondents will likely depend, in part, on when an e-mail ceases to be an electronic communication "in transit," and instead becomes a "stored electronic communication."[117] "Clearly, an opened . . . e-mail is no longer covered by the Wiretap Act."[118] But whether the act of logging onto an e-mail service provider's website without reading new e-mails is enough to move these communications out from under Wiretap Act protections is an issue yet to be decided. The earlier e-mails are no longer considered to be "in transit" and are instead considered "stored electronic communications," the fewer privacy protections they will be afforded.

---

[113] 18 U.S.C. § 2511(2)(a)(i) (2000).

[114] *See, e.g.*, Electronic Privacy Information Council, *Gmail Privacy Page*, http://www.epic.org/privacy/gmail/faq.html (last visited Jan. 4, 2005) (Section 2.4 states that "[f]rom a technical standpoint, there is no categorical difference between Google 'content extraction' and spam filtering – each involves an automated process that analyzes the body and/or header information of e-mail messages.").

[115] 18 U.S.C. § 2511(2)(a)(i).

[116] *See* Gmail Terms of Use, http://mail.google.com/mail/help/terms_of_use.html (last visited May 18, 2007); *see also* Gmail Privacy Policy, http://gmail.google.com/mail/help/privacy.html (last visited May 18, 2007) (describing Google's practice of "maintain[ing] and process[ing] your Gmail account and its contents to provide . . . relevant advertising"). A subscriber's Gmail account contents could certainly include e-mails from non-Gmail accounts. *Id.*

[117] *Compare* 18 U.S.C. § 2511(1) (prohibiting interception of electronic communications in transit), *with* 18 U.S.C. § 2701(a) (prohibiting unauthorized access to wire and electronic communications in electronic storage), *and* United States v. Councilman, 418 F.3d 67, 80–81 (1st Cir. 2005) (noting that stored electronic communications are not protected by the Wiretap Act).

[118] Center for Democracy & Technology, *supra* note 21.

If unopened e-mails are considered "stored electronic communications" when a subscriber logs onto a service provider's website, then Google's use of Adsense will probably not violate any Wiretap Act prohibitions.[119] If, however, e-mails must be opened (i.e., read) to become "stored electronic communications," it may be argued that Gmail scans are an interception in violation of the Wiretap Act.

Again, it should be noted that individuals sending e-mail from their Gmail account have consented to having their e-mails scanned.[120] But replies to these e-mails, and e-mails sent from non-Gmail accounts, are composed by individuals who have not consented to having their e-mails scanned.[121] Moreover, a non-Gmail user may not be aware that his addressee is using Gmail; many Gmail subscribers forward e-mails from other accounts to their Gmail account.[122]

Some commentators suggest that Gmail has been unfairly targeted by privacy advocates and legislators.[123] However fair or unfair this criticism, Gmail offers numerous benefits that have not been matched by its competitors, and Gmail subscribers number in the millions.[124] Whether or not Gmail intercepts electronic communications in violation of the Wiretap Act will depend in part on the reasoning adopted by courts considering the question. Courts adopting the First Circuit interpretation of the Wiretap Act are more likely to find that scanning e-mail from non-consenting users with the purpose of delivering targeted advertising is a prohibited interception under the Act, while courts adopting the narrow Fifth Circuit definition of "intercept" would likely not find such a violation.[125]

---

[119] Assuming unopened e-mails are indeed "stored electronic communications," one author has suggested that the Stored Communications Act be amended to allow interception of e-mail by the service provider only when doing so does not monetarily benefit the service provider. Jason Isaac Miller, *"Don't Be Evil": Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-mail Privacy Rights*, 33 HOFSTRA L. REV. 1607, 1640 (2005).

[120] *See id.*

[121] *See id.*

[122] *See, e.g.*, *id.* at 1609 (noting that "[e]-mail forwarding has become a widely used practice due to the number of individuals who maintain multiple e-mail accounts").

[123] *See, e.g.*, Grant Yang, *Stop the Abuse of Gmail!*, 2005 DUKE L. & TECH. REV. 14, 34–36 (2005) (suggesting that Gmail's practices are consistent with those of its competitors and with industry standards).

[124] *See* Flynn, *supra* note 112, at 16.

[125] *See supra* Parts II.B and III.

C. Voice over Internet Protocol

A related privacy issue is emerging with consumer use of Voice over Internet Protocol (VoIP) set to grow rapidly.[126] Essentially, VoIP enables individuals to use the Internet to make telephone calls.[127] Although a decade old,[128] adoption of VoIP had been hampered because it requires broadband Internet to operate properly.[129] With the increasing adoption by consumers of broadband Internet access, which includes cable modems and digital subscriber lines, use of VoIP is expected to grow rapidly.[130] According to a recent survey released by Nielsen/NetRatings, broadband use by Americans increased sixteen percent from January 2005 to August 2005, and the number of Americans with broadband access is now over 120 million, or forty-two percent of the U.S. population.[131] Furthermore, this trend is likely to continue as providers lower the cost for broadband.[132] In the United States, cable VoIP subscribers grew from 911,000 in March 2005 to 1.38 million by the end of June 2005, and analysts predict that there will be approximately four million VoIP subscribers by the end of 2005.[133] That number is expected to increase to over seventeen million in the next few years.[134] In addition to lower cost as compared with traditional phone service, use of VoIP carries with it the possibility of attaching documents, video, and other data to a phone call.[135]

Traditional telephone systems connect calls using a system known as circuit switching.[136] When a call is made, this method main-

---

[126] *See* Jon Van, *VoIP Moves Beyond Blip Stage; Site Reviews Providers*, CHI. TRIB., Mar. 6, 2006, at 6.

[127] *See id.*

[128] Intertangent Technology Directory, *History of VoIP*, http://www.intertangent.com/023346/Articles_and_News/1413.html (last visited Oct. 19, 2005).

[129] *See* Paul Taylor, Mark Odell & Michiyo Nakamoto, *Why VoIP Telephony Is Quickly Coming of Age*, FIN. TIMES, Sept. 8, 2005, *available at* www.westlaw.com, 2005 WLNR 14151006.

[130] *Id.*

[131] Press Release, Nielsen/NetRatings, Two Out of Every Five Americans Have Broadband Access at Home (Sept. 28, 2005), *available at* http://www.netratings.com/pr/pr_050928.pdf.

[132] *Id.*

[133] Taylor, *supra* note 129.

[134] *Id.*

[135] *See, e.g.*, Owen D. Kurtin & Arthur S. Katz, *Has Internet-Based Phone Calling Outpaced the Law?: A Hands-Off Regulatory Approach Fostered VoIP, but Its Competitors Are Highly Regulated. What Should Be Done?*, 27 LEGAL TIMES 45 (describing as "revolutionary" the possibilities associated with VoIP).

[136] VoIP: Circuit Switching and Packet Switching, http://computer.howstuffworks.com/ip-telephony2.htm (last visited Apr. 19, 2007).

tains a connection, known as a circuit, between the parties for as long as they both remain on the line.[137] While dependable, this method is inefficient because much of the data transmitted during a telephone call is wasted.[138] In contrast, VoIP technology utilizes a more efficient method to transmit data, known as packet switching.[139] While circuit switching maintains a constant connection, packet switching opens a connection just long enough to send a small amount of data, known as a packet, from one computer to another.[140] The data transmission is similar to that of e-mails, with individual data packets sent along the least congested route before being reassembled at their destination.[141]

However, the same technological aspects of VoIP that make it efficient also raise significant concerns about the privacy of these communications, an issue that neither the courts nor Congress have yet addressed. Although a complete discussion of the legal issues related to VoIP is beyond the scope of this Comment, one important privacy-related issue is worth noting.

It would appear that VoIP communications could reasonably be classified as either a "wire communication," like a traditional telephone call, or as an "electronic communication" under the Wiretap Act.[142] The technical aspects of VoIP make the transmission seem similar in many respects to the transmission of e-mail and other "electronic communication[s]."[143] Furthermore, the Act's definition of "electronic communication" includes "any transfer of . . . sounds."[144] However, it seems more likely that courts will, at least initially, classify VoIP communications as "wire communications" for two reasons. First, despite its technical aspects, a VoIP communication remains an "aural transfer," and remains, in essence, a telephone call.[145] Second, the House report concerning the ECPA made Congress's intentions clear when it stated that "[a]s a rule, a communication is an electronic communication if it . . . [cannot] fairly be characterized as one

---

[137] *Id.*

[138] *Id*

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] *See supra* notes 82–84 and accompanying text.

[143] *Compare* VoIP: Circuit Switching and Packet Switching, *supra* note 136 (explaining the difference between traditional telephone systems and the VoIP system), *with* 18 U.S.C. § 2510(12) (2000) (defining "electronic communication").

[144] § 2510(12).

[145] *See* § 2510(1).

containing the human voice."[146] Thus, it seems that the most logical classification for VoIP would be as a "wire communication," providing the same level of privacy protections that traditional telephone calls enjoy.

Assuming that courts do find VoIP to be a "wire communication," the USA PATRIOT Act's amendment to the definition of "wire communication" again becomes troubling.[147] The amendment supports the argument that while VoIP communications in transit are covered by the Wiretap Act, VoIP communications in storage, including the transient storage associated with the transfer of these communications, are afforded only the less robust protections of the Stored Communications Act.

V. STRATEGIES TO IMPROVE THE PRIVACY OF INTERNET COMMUNICATION

Existing law is ill-suited to protect many forms of Internet-based communication. Written at a time when recent technological advances and widespread use of the Internet as a means to communicate could not have been foreseen,[148] portions of the Wiretap Act are now obsolete and inadequate to protect the privacy of Internet communication. As the district court in the *Councilman* decision observed, "technology has, to some extent, overtaken language. Traveling the Internet, electronic communications are often—and perhaps constantly—both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox."[149] The distinction between communications "in transit" and communications "in storage" is no longer relevant. This distinction could be eliminated by either legislative or judicial action. As this Part will suggest, the best way to ensure the privacy of Internet communications is to enact specific legislation.

Before proceeding, a short introduction to a currently available judicial—and legislative—independent solution is appropriate. In the absence of a comprehensive statute, individuals can be proactive in protecting their Internet communications by adopting encryption technologies. One popular program that can be used to encrypt e-mail messages is Pretty Good Privacy (PGP).[150] PGP uses "public key

---

[146] *Councilman II*, 418 F.3d at 77 (quoting H.R. REP. NO. 99-647, at 35 (1986)).

[147] *See supra* notes 103–07 and accompanying text.

[148] *See supra* Part II.A.

[149] United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003).

[150] PGP software can be downloaded as freeware for noncommercial use from www.pgpi.com.

cryptography" to generate two keys: a public key to encrypt data, and a private key for decryption.[151] The public key, as its name suggests, may be distributed to anyone with whom an individual corresponds, while the private key is kept secret.[152] Individuals can then use the public key to encrypt e-mails that only a recipient with the private key can read.[153] Encryption software is also available for instant messaging, and the creator of PGP recently created a prototype to be used with VoIP.[154]

While it is a somewhat cumbersome solution, a good encryption program is effective against all but the most determined attackers.[155] Additionally, even the most comprehensive statute can only establish what conduct is permissible in regard to third party access to Internet communication; it cannot itself prevent impermissible conduct. Furthermore, as a result of the rapidity with which communication technology is presently advancing, any governing statutes will likely be reactive rather than proactive.[156] Encryption is a solution that protects communication privacy against unscrupulous conduct, whether or not an existing statute prohibits that conduct.

As noted, however, encryption technologies can be cumbersome and confusing, and this drawback has prevented their widespread adoption.[157] The creator of PGP has himself described the program as "not that easy to use"[158] and noted that "[w]e'll be better off if we develop a system that your mom can use."[159] Regardless of whether such a system is ever developed, Congress and the courts should work to protect the privacy of Internet communications.

A. Judicial Solution

Both narrow and broad judicial solutions that would protect Internet communications have been proposed.[160] The narrow solu-

---

[151] PGP Corporation, *An Introduction to Cryptography* 12 (June 8, 2004) (on file with author).

[152] *Id.*

[153] *Id.*

[154] *See* Kim Zetter, *Privacy Guru Locks Down VoIP*, WIRED NEWS, July 26, 2005, http://www.wired.com/news/technology/0,1282,68306,00.html.

[155] *See* Michael Cohn, *7 Myths About Network Security: The Only Way to Keep Data Safe May Be to Stay One Step Ahead of Hackers*, INS. & TECH., June 1, 2005, at 41.

[156] *See generally* Campbell, *supra* note 10.

[157] *See* Michael Bazeley, *Building a Useful Wall: Internet Users Can Reclaim Some Privacy from the Unscrupulous*, CHARLESTON GAZETTE, May 4, 2003, at 6D.

[158] *Id.*

[159] *Id.*

[160] *See* Campbell, *supra* note 10, at 542–47.

tion consists of "looking to congressional intent to fill in gaps in the wiretapping laws,"[161] so that Internet communications are given an appropriate level of protection. However, numerous circuit courts have rejected this approach, making it "unlikely that [this] approach would be uniformly adopted."[162]

The broad judicial solution would protect communications generally, including Internet communications, and would be based on existing Constitutional and tort concepts—the Fourth Amendment and the tort of invasion of privacy.[163] In his dissent in *Olmstead v. United States*,[164] Justice Brandeis stated:

> The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[165]

Additionally, "[c]ourts have already found liability for wiretapping under the 'unreasonable intrusion' rubric of invasion of privacy."[166] By drawing on the "unreasonable intrusion" ground and Justice Brandeis's language, it is suggested that "[i]t would be only a small step to add Internet-based communications to the protected class of communications."[167]

B. Legislative Solution

In the United States, no comprehensive law protects privacy rights.[168] Instead, "[p]rivacy rights arise from a patchwork of constitutional rights, common law rights, and federal, state, and local laws."[169]

---

[161] *Id.* at 542–43.

[162] *Id.* at 543. Campbell notes that the "First, Third, Fifth, Ninth, and Eleventh Circuit Courts of Appeal have found areas in which the current wiretapping laws do not protect communications." *Id.* at 538. Additionally, Campbell suggests that perhaps the best scenario would be that a circuit split develops, which the Supreme Court may resolve "in favor of using congressional intent to fill in the wiretapping law's gaps." *Id.* at 543.

[163] *Id.*

[164] 277 U.S. 438 (1928).

[165] *Id.* at 478 (Brandeis, J., dissenting).

[166] Campbell, *supra* note 10, at 544.

[167] *Id.*

[168] Suzanne Ross McDowell, *Nonprofits and the Internet: Tax and Other Legal Issues*, 21 No. 10 COMPUTER & INTERNET LAW. 21, 34 (2004).

[169] *Id.*

A 1998 Federal Trade Commission Report to Congress described "American privacy law . . . as sectoral, consisting of a handful of disparate statutes directed at specific industries."[170] Some of these statutes are specific to Internet privacy, but many are not.[171] There are two specific steps that Congress could take to remedy this shortcoming in the law.

First, Congress should eliminate the current storage-transit dichotomy that exists in relation to the transmission of Internet communications. Internet communications should be afforded the same level of protection regardless of whether they are in transit or in the type of transient storage associated with the store-and-forward method of Internet communications. Furthermore, Congress should amend the Wiretap Act's definition of "electronic storage" to eliminate any possibility that the definition could be interpreted as applying to electronic communications in the type of transient storage incidental to store-and-forward transmission.

In reaction to the panel decision in *Councilman I*, Vermont's Senator Leahy and New Hampshire's Senator Sununu introduced the E-Mail Privacy Act of 2005.[172] This legislation would amend the definition of "intercept" in the Wiretap Act to read: "'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication contemporaneous with transit, or on an ongoing basis during transit, through the use of any electronic, mechanical, or other device or process, notwithstanding that the communication may simultaneously be in electronic storage."[173] This proposal is essentially a codification of the holding in *Councilman II* and would eliminate both the dichotomous treatment of interceptions of wire and electronic communications and the distinction between electronic communications in transit and those in transient storage.

---

[170] MARTHA K. LANDESBERG ET AL., PRIVACY ONLINE: A REPORT TO CONGRESS 62 n.160 (1998). The report also lists a number of federal statutes governing privacy rights in specific industries. *Id.* *See also* Richard D. Marks, *Security, Privacy, and Free Expression in the New World of Broadband Networks*, 32 HOUS. L. REV. 501, 503 (1995) (noting that current federal statutes governing privacy form a "haphazard" pattern) (quoting Darryl C. Wilson, *Viewing Computer Crime: Where Does the Systems Error Really Exist?*, 11 COMPUTER/L.J. 265, 265 (1991)).

[171] *See* LANDESBERG ET AL., *supra* note 170, at n.160.

[172] S. 936, 109th Cong. (2005).

[173] *Id.* at § 2. As currently written, the Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (2000).

The Wiretap Act currently defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[174] The problem with this definition is that, as shown by *Councilman II*, it can be interpreted to create an overlap between the Wiretap Act and the Stored Communications Act.[175] That is, a violation of the Wiretap Act can sometimes occur when a stored electronic communication is intercepted.[176] And although the court's reasoning is true to the Wiretap Act's purpose, one can credibly argue that it is technically incorrect.[177]

The "temporary, intermediate storage" in the definition of "electronic storage" was intended to describe back-up storage, or storage that occurs when an electronic communication is undeliverable, not storage that occurs while a communication is en route from sender to recipient.[178] However, Internet communications do indeed undergo "temporary, intermediate storage" during transmission, and the *Councilman I* court relied heavily on this phenomenon in concluding that there could be no violation of the Wiretap Act because the e-mails were taken from electronic storage.[179]

The definition of "electronic storage" should be changed to complement the Leahy-Sununu amendment and to reflect the idea that Internet communications in transit are at no time during transmission in "electronic storage" for purposes of the Wiretap Act. Drawing on language currently employed, a potential amendment could read:

> (1) "electronic storage" means –
>
> > (A) any storage of a wire or electronic communication subsequent to the electronic transmission thereof; and
> > (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; but does not include

---

[174] § 2510(17).

[175] *See Councilman II*, 418 F.3d at 80–82.

[176] *See id.*

[177] *See id.* at 85–88 (Torruella, J., dissenting). In his dissent, joined by Senior Circuit Judge Cyr, Judge Torruella argued that a strict construction of the term "electronic storage" necessitated a conclusion that Councilman could not have violated the Wiretap Act. *Id.* (Torruella, J., dissenting).

[178] *See, e.g.*, Mulligan, *supra* note 9, at 1568–69.

[179] United States v. Councilman (*Councilman I*), 373 F.3d 197, 202–04 (1st Cir. 2004).

> (C) transient, momentary storage incidental to electronic communication transmissions employing electronic communications systems.[180]

The above amendment to the definition of "electronic storage," combined with enactment of the E-Mail Privacy Act of 2005, will hopefully ensure Internet communications' inclusion within the protections of the Wiretap Act when the communications are en route from sender to recipient.

VI. CONCLUSION

Despite the potential privacy threats associated with their use, Internet communication technologies will continue to be employed by an ever-increasing number of individuals. Attracted by the technological efficiency, convenience, and potential for cost savings, the majority of people who communicate using the Internet likely do so without much thought for the privacy of their communications. As is true with many of the rights we enjoy, most people do not seem to be concerned about their right to privacy until it has been violated.[181]

The decision in *Councilman II* was undoubtedly a step in the direction toward protecting the privacy of Internet communications. It was, however, a small step. Limited to its rather unusual and technical facts, the court's decision is unlikely to have a substantial impact on Internet communication privacy. Until other courts adopt the reasoning of *Councilman II*, any effect the decision does have will be felt in only a few states in New England.

Unfortunately, there seems to be no panacea to guard against Internet communication privacy threats.[182] While individuals should be proactive in protecting the privacy of their online communications by adopting simple encryption technologies to ensure that communications they wish to be private are so, legislation is the best way to ensure the privacy of Internet communications. Hopefully, Congress will soon see fit to enact legislation that not only ensures that currently existing rights remain intact, but also will undo the effects of what many feel have been unduly narrow interpretations of laws cited by those seeking to protect their privacy.

---

[180] "Electronic communications system" is defined in 18 U.S.C. § 2510(14) (2000).

[181] *See, e.g.*, ROBERT O'HARROW, JR., NO PLACE TO HIDE 74–83 (2005).

[182] *See supra* notes 168–71 and accompanying text.